УДК 343.102

К. С. Малышев
преподаватель кафедры оперативно-разыскной деятельности органов внутренних дел Уральского юридического института МВД России

ОСОБЕННОСТИ ПРОВЕДЕНИЯ ОПЕРАТИВНО-РОЗЫСКНОГО МЕРОПРИЯТИЯ «ПОЛУЧЕНИЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ» ПРИ РАСКРЫТИИ ЛАТЕНТНОЙ ПРЕСТУПНОСТИ

В статье анализируются понятие, содержание оперативно-розыскного мероприятия (далее — ОРМ) «получение компьютерной информации», а также отдельные аспекты и практические особенности проведения данного мероприятия при раскрытии латентной преступности.

В настоящее время с преобладанием в нашей жизни информационно-коммуникационных технологий, с незаменимым в использовании феноменом под названием глобальная сеть Интернет появилась почва для развития такого криминального аспекта, как латентная преступность или, проще говоря, мошенничество, которое осуществляется с использованием сети Интернет. Ежегодно показатель данной группы преступлений растет и появляются более усовершенствованные схемы преступной деятельности.

Мошенники были, есть и будут во все времена. На Руси 700 лет назад местные жители называли вора «посак». Данное слово через некоторое время нашли ученые на берестяной грамоте, найденной в Великом Новгороде и датированной первой половиной XIV века. Это подтверждает тот факт, что издавна обманывали людей с целью получения материальной или иной выгоды различными способами.

С появлением широкой и доступной для всех глобальной сети Интернет и внедрением в нашу жизнь информационных технологий этот вид хищения стал популярен. Интернет для мошенников представляет массу возможностей:

Во-первых, множество пользователей не обладают достаточными знаниями в области интернет-технологий и интернет-мошенничества.

Во-вторых, мошенники широко используют кибер-технологии, которые помогают им получать доступ к данным граждан.

В ходе практической деятельности формально выделяют определенные черты получаемой информации о фактах преступлений, совершаемых в сфере высоких технологий: устойчивость, латентность и т. д.

Данная группа преступлений в силу своей латентности становится неуязвимой и нередко в раскрытии и расследовании мошенничества возникают

сложности из-за невозможности установить преступника, совершившего данное преступление.

Именно из-за анонимности, сложности нахождения преступников, а иногда даже невозможности их выявления оперативно-розыскными подразделениями данный вид преступления расследуется весьма проблематично.

Компьютерной информации отведена значимая роль при решении вопроса о возбуждении уголовного дела и дальнейшего обеспечения процесса доказывания.

Учитывая данные условия и аспекты в оперативно-розыскной практике, возникла необходимость найти наиболее эффективный способ борьбы с данным видом преступлений.

С целью законодательного урегулирования получения информации, находящейся в современных компьютерных системах, был введен Федеральный закон от 6 июля 2016 г. № 374-ФЗ «О внесении изменений в Федеральный закон “О противодействии терроризму” и отдельные законодательные акты Российской Федерации».

Необходимо сначала разобраться в составляющих данной дефиниции. Так, в ст. 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» дается общее понятие информации: это сведения (сообщения, данные), независимо от формы их представления.

В уголовном законодательстве (примеч. 1 к ст. 272 УК РФ) под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Обратимся к определениям понятия «получение компьютерной информации».

Исследовав эмпирические материалы, можно сделать вывод о специфической характеристике, присущей каждому понятию: все они сопоставимы с определением «компьютерная информация» в соответствии с законодательным закреплением.

Возможно получение компьютерной информации в целях получения виртуальных данных, содержащихся на жестком диске компьютера или периферийных электронных устройств, а кроме того, получение данных, находящихся в «облачном» сервере, если свободный доступ к ней ограничен.

Данное мероприятие имеет высокое практическое значение, так как с его помощью возможно получать необходимую информацию по средствам удаленного доступа к компьютерной техники и различным серверам Интернета.

Проблемой осуществления данного ОРМ является наличие ограниченности по отношению к конституционным правам и свободам граждан, ведь его реализация непосредственно затрагивает права на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи.

Данное ОРМ выполняется посредством специальных технических устройств. Информация, полученная в ходе данного ОРМ, имеет важное значение для дальнейшего расследования уголовного дела и процесса доказывания.